UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/992,310	11/19/2001	Laurence I. Rockwell	7784-000188	7369

27572 7590 07/29/2004

HARNESS, DICKEY & PIERCE, P.L.C.
P.O. BOX 828
BLOOMFIELD HILLS, MI 48303

EXAMINER	
PEACHES, RANDY	

ART UNIT	PAPER NUMBER
2686	8

DATE MAILED: 07/29/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/992,310	ROCKWELL, LAURENCE I.	
	Examiner	Art Unit	
	Randy Peaches	2686	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-19 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-19 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date 2&3- 6/3,6/23/03.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Specification

Applicant is reminded of the proper language and format for an abstract of the disclosure.

The abstract should be in narrative form and generally limited to a single paragraph on a separate sheet within the range of 50 to 150 words. It is important that the abstract not exceed 150 words in length since the space provided for the abstract on the computer tape used by the printer is limited. The form and legal phraseology often used in patent claims, such as "means" and "said," should be avoided. The abstract should describe the disclosure sufficiently to assist readers in deciding whether there is a need for consulting the full patent text for details.

The language should be clear and concise and should not repeat information given in the title. It should avoid using phrases which can be implied, such as, "The disclosure concerns," "The disclosure defined by this invention," "The disclosure describes," etc.

The Applicant is reminded that the Abstract should contain a maximum of 150 words. The Examiner suggests that the submitted Abstract be amended to reflect the above requirement.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

1. ***Claims 1, 5, 7, 9, 11-12, 15, 17 and 19*** are rejected under 35 U.S.C. 102(e) as being anticipated by Monroe (U.S. Patent Number 6,392,692 B1).

Regarding ***claims 1, 12 and 19***, Monroe discloses in column 11 lines 5-6, of a comprehensive surveillance system for tracking, and/or surveillance of aircraft, ships, and other commercial vehicles, hereinafter referenced collectively as "commercial vehicles", which reads on claimed "network security architecture for monitoring security activities in a mobile network platform", comprising:

- a safety and surveillance equipment (transport installed system), which reads on claimed "mobile network", as taught in column 1 lines 25-30, residing on the said commercial vehicles, which reads on claimed "mobile network platform", the said transport installed system being interconnected via a link to the ground station or personal security unit, as disclosed in column 2 lines 46-48, 56-61, which reads on claimed "terrestrial-based network security management system";

- a aircraft sensor system (see column 3 lines 19-24), which reads on claimed "intrusion detection system", connected to the said transport installed system and residing on the said commercial vehicle, the said sensor system operable to detect a breach of security, unexpected event , or other unusual activities, which reads on claimed "security intrusion event", that is associated with the said transport installed system. See column 3 lines 9-15;
- a comprehensive multi-media system, which reads on claimed "mobile security manager", residing on the said commercial vehicle and adapted with a data collection scheme for safety and surveillance (column 3 lines 31-35) from the said sensor system, which reads on claimed "adapted to receive the security intrusion events from the intrusion detection system", the said comprehensive multi-media system is further operable to respond to the crew members and ground station, when applicable, which reads on claimed "security response", to the said breach of security events, when the said commercial vehicle is not connected with a said ground station, which reads on claimed "not connected", with the network security management system. See column 4 lines 36-39.

Regarding ***claims 5 and 15***, according to ***claims 1***, Monroe continue to teach wherein the said comprehensive surveillance system is comprised wherein the said transport installed system includes a plurality of sensors, which reads on claimed "plurality of user access points", such that the said breach of security is associated with one of the said

plurality of sensors and the said response is directed to said one of the plurality of sensors, as disclosed in column 16 lines 28-36.

Regarding ***claims 7 and 17***, according to ***claims 5 and 15***, Monroe continue to teach herein the said comprehensive multi-media system maintains an indicator of the current operational state for each of the plurality of said sensors, such that the security response directed to said one of the plurality of said sensors is in part based on the operational state of said one of the plurality of user sensors. See column 14 lines 51-61.

Regarding ***claim 9***, according to ***claim 7***, Monroe continue to teach wherein the said comprehensive multi-media system is further operable to identify the current operational state for said one of the plurality of said sensors and perform security response activities based in part on the identified operational state and the security intrusion event received from the intrusion detection system. See column 18 lines 4-12, 34-42.

Regarding ***claim 11***, according to ***claim 1***, Monroe continue to teach wherein the said comprehensive multi-media system is operable to transmit a message indicative of the security intrusion event to the said ground station or personal security unit and to perform security response activities in response to security commands received from the said comprehensive multi-media system. See column 8 lines 18-36 and column 17

lines 16-31.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. ***Claim 2-3 and 13*** are rejected under 35 U.S.C. 103(a) as being unpatentable over Monroe (U.S. Patent Number 6,392,692 B1) in view of Manganaris et al (U.S. Publication Number 2002/0082886 A1).

Regarding ***claims 2 and 13***, according to ***claims 1 and 13***, Monroe discloses in column 11 lines 5-6, of a comprehensive surveillance system for tracking, and/or surveillance of aircraft, ships, and other commercial vehicles, hereinafter referenced collectively as "commercial vehicles", which reads on claimed "network security architecture for monitoring security activities in a mobile network platform", comprising:

- a safety and surveillance equipment (transport installed system), which reads on claimed "mobile network", as taught in column 1 lines 25-30, residing on the said commercial vehicles, which reads on claimed "mobile network platform", the said transport installed system being interconnected via a link to the ground station or

personal security unit, as disclosed in column 2 lines 46-48, 56-61, which reads on claimed "terrestrial-based network security management system";

- a aircraft sensor system (see column 3 lines 19-24), which reads on claimed "intrusion detection system", connected to the said transport installed system and residing on the said commercial vehicle, the said sensor system operable to detect a breach of security, unexpected event , or other unusual activities, which reads on claimed "security intrusion event", that is associated with the said transport installed system. See column 3 lines 9-15;
- a comprehensive multi-media system, which reads on claimed "mobile security manager", residing on the said commercial vehicle and adapted with a data collection scheme for safety and surveillance (column 3 lines 31-35) from the said sensor system, which reads on claimed "adapted to receive the security intrusion events from the intrusion detection system", the said comprehensive multi-media system is further operable to respond to the crew members and ground station, when applicable, which reads on claimed "security response, to the said breach of security events, when the said commercial vehicle is not connected with a said ground station, which reads on claimed "not connected with the network security management system. See column 4 lines 36-39.

However, Monroe does not expressively disclose wherein a comprehensive surveillance system is operable perform security response activities in accordance with a security policy resident on the mobile network platform.

Manganaris et al teaches of an automated decision engine, which reads on claimed "security policy resident", operable to screen incoming alarms and according to conditions and trigger an alarm, which reads on claimed "security response activities", to alert others of the unusual behaviors. See paragraph [0013].

Therefore, at the time of the invention it would have been obvious to a person of ordinary skilled in the art to modify Monroe (U.S. Patent Number 6,392,692 B1) to include Menard et al (U.S. Publication Number 2002/0177428 A1) in order to implement a functional element of the said system that determines the response according to the incoming alarm for a particular alarm event.

Regarding ***claim 3***, as the above combination of Monroe (U.S. Patent Number 6,392,692 B1) in view of Manganaris et al (U.S. Publication Number 2002/0082886 A1) are made, the combination according to ***claim 2***, further teaches, as disclosed by Manganaris et al in paragraph [0022], of a series of event alarms and/or event groupings or a combination of single events or event bursts, which reads on claimed "plurality of pre-defined security intrusion events", and in response to the said events being recognized as unusual, then a triggered alarm is created, which reads on claimed "security response for each of said plurality of security intrusion events", to alert others of the unusual behavior.

3. ***Claim 4*** is rejected under 35 U.S.C. 103(a) as being unpatentable over Monroe (U.S. Patent Number 6,392,692 B1) in view of Manganaris et al (U.S. Publication

Number 2002/0082886 A1) in further view of Schuba et al (U.S. Patent Number 6,725, 378 B1).

Regarding ***claim 4***, as the combination of Monroe (U.S. Patent Number 6,392,692 B1) and Manganaris et al (U.S. Publication Number 2002/0082886 A1) are made, the combination according to ***claim 2***, fails to discloses wherein data structure having a current operational state element, a possible security intrusion event element, a resulting operational state element, and a security response element.

Schuba et al discloses in column 8 lines 5-49, of classification operation of perfect, evil and suspect, which reads on claimed "a possible security intrusion event element, a resulting operational state element, and a security response element.

Therefore, at the time of the invention it would have been obvious to a person of ordinary skilled in the art to modify the combination of Monroe (U.S. Patent Number 6,392,692 B1) and Manganaris et al (U.S. Publication Number 2002/0082886 A1) to further include Schuba et al (U.S. Patent Number 6,725, 378 B1) in order define the effective operational states of an intrusion event to ensure a proper response is taken in effect.

4. ***Claims 6, 10 and 16*** are rejected under 35 U.S.C. 103(a) as being unpatentable over Monroe (U.S. Patent Number 6,392,692 B1) in view of ISA ***"An Introduction to Intrusion Detection Assessment for System and Network Security Management".***

Regarding ***claims 6 and 16***, according to ***claims 5 and 15***, Monroe discloses where the said comprehensive surveillance system is comprised wherein the said transport installed system includes a plurality of sensors, which reads on claimed "plurality of user access points", such that the said breach of security is associated with one of the said plurality of sensors and the said response is directed to said one of the plurality of sensors, as disclosed in column 14 lines.

Monroe continues to disclose where the pre-selected alarm signals are transmitted to the respected response center handling the breach of security notification. See column 18 lines 34-42. Additionally, provides a warning signal, which reads on claimed "warning message", to at least one of the said sensors, providing a said warning signal to the said network security management system.

However, Monroe does not disclose wherein installing a network traffic blocking filter at one of said user access points, and disconnecting one of said user access points from the mobile network.

ISA discloses on page 29 under topic *Alter the Environment*, wherein at the time of a said breach of security, a network alteration can consist of blocking access to the user from the same source address, which reads on claimed " traffic blocking filter at one of said user access points, and disconnecting one of said user access".

Therefore, at the time of the invention it would have been obvious to a person of ordinary skilled in the art to modify Monroe (U.S. Patent Number 6,392,692 B1) to include ISA ***"An Introduction to Intrusion Detection Assessment for System and Network Security Management"*** in order to provide a system capable to filtering user's access to the network when a said breach of security id evident.

Regarding ***claim 10***, according to ***claim 9***, Monroe continues to teach wherein the said comprehensive multi-media system is further operable to identify the current operational state for said one of the plurality of said sensors and perform security response activities based in part on the identified operational state and the security intrusion event received from the intrusion detection system. See column 18 lines 4-12, 34-42.

However, Monroe does not disclose wherein the operational states of the said sensors are changed by the said comprehensive multi-media system.

ISA discloses on page 29 under topic *Alter the Environment*, wherein at the time of a said breach of security, a network alteration can consist of blocking access to the user from the same source address, which reads on claimed " traffic blocking filter at one of said user access points, and disconnecting one of said user access".

Therefore, at the time of the invention it would have been obvious to a person of ordinary skilled in the art to modify Monroe (U.S. Patent Number 6,392,692 B1) to include ISA ***"An Introduction to Intrusion Detection Assessment for System and Network Security Management"*** in order to provide a system capable to changing the

operational state of a said sensor to either the security level or increase dependent on the said security policy.

5. ***Claims 8, 14 and 18*** are rejected under 35 U.S.C. 103(a) as being unpatentable over Monroe (U.S. Patent Number 6,392,692 B1) in view of Schuba et al (U.S. Patent Number 6,725, 378 B1).

Regarding ***claims 8 and 18***, according to ***claims 7 and 17***, Monroe fails to teach wherein the current operational state for any given access point is selected from the group consisting of a normal state, a suspended state, and a disconnect state.

Schuba et al teaches in column 8 lines 5-49 where three alarm classifications are disclosed: perfect, evil and suspect, which reads on claimed " normal state, a suspected state, and a disconnect state". Of which, each represents a different function as to the reaction the said system will take when the said alarm condition is present.

Therefore, at the time of the invention it would have been obvious to a person of ordinary skilled in the art to modify Monroe (U.S. Patent Number 6,392,692 B1) to include Schuba et al (U.S. Patent Number 6,725, 378 B1) in order to define a security event hierarchy to ensure a proper operational state for the said sensors.

Regarding ***claim 14***, according to ***claim 12***, Monroe fails to disclose wherein the security policy is defined by a data structure having a current operational state element,

a possible security intrusion event element, a resulting operational state element, and a security response element.

Schuba et al discloses in column 8 lines 5-49, of classification operation of perfect, evil and suspect, which reads on claimed "a possible security intrusion event element, a resulting operational state element, and a security response element.

Therefore, at the time of the invention it would have been obvious to a person of ordinary skilled in the art to modify Monroe (U.S. Patent Number 6,392,692 B1) to include Schuba et al (U.S. Patent Number 6,725, 378 B1) in order to order define the effective operational states of an intrusion event to ensure a proper response is taken in effect.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Randy Peaches whose telephone number is (703) 305-8993. The examiner can normally be reached on Monday - Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Marsha D. Banks-Harold can be reached on (703) 305-4379. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Randy Peaches
July 12, 2004

Nguyen Vo
7_22_04

NGUYEN T. VO
PRIMARY EXAMINER